別紙1の
対応公報
corresponding
to Ref. 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－313487

(43)公開日　平成10年(1998)11月24日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ	7/26	１０９Ｓ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ａ

審査請求　未請求　請求項の数９　ＯＬ　（全 5 頁）

(21)出願番号　特願平10－88648

(22)出願日　平成10年(1998)４月１日

(31)優先権主張番号　９７０４００１

(32)優先日　1997年４月２日

(33)優先権主張国　フランス（ＦＲ）

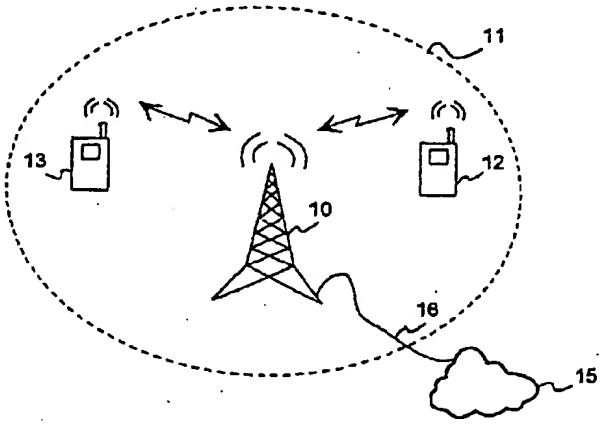
(71)出願人　590000248
コーニンクレッカ　フィリップス　エレクトロニクス　エヌ　ヴィ
Ｋｏｎｉｎｋｌｉｊｋｅ　Ｐｈｉｌｉｐｓ　Ｅｌｅｃｔｒｏｎｉｃｓ　Ｎ．Ｖ．
オランダ国　アインドーフェン　フルーネヴァウツウエッハ　1

(72)発明者　ピエール－ユーグ、ブシャール
フランス国サン、タベルタン、リュ、ド、ラルケ、19

(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　電気通信システム、移動端末、および移動端末を電気通信網に登録するための方法

(57)【要約】
【課題】　電気通信システム、移動端末、並びに、移動端末を電気通信網に登録するための方法。
【解決手段】　本発明は、少なくとも無線基地局と移動端末とを有する電気通信網に関する。本発明によると、移動端末は、電気通信網に自身を知らせるために、無線基地局に機密認証コードを送信する。本発明は、特に、移動端末を、無線基地局を介して電気通信網に登録するための、網にとって加入者の管理が容易な、登録手続きを開示する。この目的のために、機密認証コードにある期間が割当てられ、端末の登録手続きは、前記の機密認証コードを、前記の期間内の日付に供給することから成る。



1

【特許請求の範囲】

【請求項１】電気通信システムであって、このシステムが、少なくとも固定部分と、移動端末を含み、前記移動端末が、前記システムに登録するために、機密認証コードを前記固定部分に供給し、前記機密認証コードに少なくともある期間が割当てられ、前記登録手続きは、前記機密認証コードを、前記期間に応じた日付に供給することを特徴とする電気通信システム。

【請求項２】ＥＴＳＩ（欧州電気通信標準協会）３００１７５－５タイプの標準に準拠し、前記機密認証コードが、前記標準において規定されるキー割当て手順における認証コードＡＣとして用いられることを特徴とする請求項１に記載のシステム。

【請求項３】少なくとも前記移動端末が識別番号、特に、ＩＰＥＩ（国際携帯機器識別）を持ち、この機密認証コードは、前記携帯端末のＩＰＥＩと独立なことを特徴とする請求項１あるいは２のいずれか一つに記載のシステム。

【請求項４】電気通信網の固定部分に機密認証コードを供給することで電気通信網に登録して用いる移動電話端末であって、前記移動電話端末は、

前記機密認証コードにある期間が割当てられ、前記登録手続きが、前記機密認証コードを前記期間に応じた日付に供給することから成ることを特徴とする移動電話端末。

【請求項５】ＥＴＳＩ（欧州電気通信標準協会）３００１７５－５タイプの標準に準拠して動作するように意図され、前記機密認証コードが、前記標準において規定されるキー割当て手順における認証コードＡＣとして用いられることを特徴とする請求項４に記載の移動電話端末。

【請求項６】識別番号、特に、ＩＰＥＩ（国際携帯機器識別）を持ち、前記機密認証コードが、前記端末のＩＰＥＩと独立なことを特徴とする請求項４あるいは５のいずれか一つに記載の移動電話端末。

【請求項７】移動端末を機密認証コードを用いて電気通信網に登録するための方法であって、前記電気通信網が少なくとも一つの無線基地局を持ち、前記機密認証コードに期間が割当てられ、前記登録手続きが、前記無線基地局に、前記機密認証コードを前記期間に応じた日付に供給することから成ることを特徴とする登録方法。

【請求項８】ＥＴＳＩ（欧州電気通信標準協会）３００１７５－５タイプの標準に準拠して動作するように意図して移動端末を電気通信網に登録するための方法であって、前記機密認証コードが、前記標準において規定されるキー割当て手順における認証コードＡＣとして用いられることを特徴とする請求項７に記載の方法。

【請求項９】前記移動端末が、識別番号、特に、ＩＰＥＩ（国際携帯機器識別）を持ち、前記機密認証コードが、前記携帯端末のＩＰＥＩと独立なことを特徴とする

2

請求項７あるいは８のいずれか一つに記載の方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、少なくとも一つの固定部分と、電気通信システムに登録する目的でその固定部分に機密認証コードを供給するのに適した移動端末とを有する電気通信システムに関する。

【０００２】本発明は、同様に、機密認証コードを電気通信網の固定部分に供給することで電気通信網に登録して用いられる移動電話端末に関する。

【０００３】本発明は、最後に、移動端末を、機密認証コードを介して、少なくとも一つの無線基地局を含む電気通信網に登録するための方法に関する。

【０００４】本発明は、移動無線電気通信の分野、特に、ＤＥＣＴ（デジタル・エンハンスド・コードレス電気通信）の分野に有効な用途を持つ。本発明は、移動電話網のユーザの管理を、例えば、移動電話網のユーザが網あるいは網の特定のサービスに加入する際の、無線基地局への登録を簡素化することで、容易にするための手段を提供する。

【０００５】

【従来の技術】米国特許第5,077,790号は、移動端末を、コードレス電話網に登録するための方法を開示する。この方法によると、コードレス電話網は、網コントローラを含み、網コントローラは、網内の既知の携帯端末の識別番号を含むデータベースを有する。登録に当たって、携帯端末は、網の基地局に、携帯端末の識別番号を含む登録リクエストを送る。網コントローラは、こうして送られた識別番号が網コントローラのデータベース内に見つかった場合は、リクエストに対して肯定的な返事を送る。

【０００６】

【発明が解決しようとする課題】網に携帯端末を登録するための上述の方法は、番号を、順番に、データベース内に含まれる全ての番号と比較することを要求され、このために、実現および管理が困難である。

【０００７】本発明の一つの目的は、この困難を克服し、移動電話網のユーザが網あるいは網の特定のサービスに加入する際の、移動電話網のユーザの識別を管理するための、実現および管理が簡単な、単純な手段を提供することにある。

【０００８】

【課題を解決するための手段】本発明は、冒頭の段落において規定される電気通信システム、携帯端末および携帯端末を電気通信網に登録するための方法であって、前記機密認証コードに少なくともある期間が割当てられ、前記登録手続が、前記期間に応じた日付で前記機密認証コードを供給することを特徴とする。

【０００９】本発明の一つの好ましい実施例においては、ある期間に対して、その期間に割当てられた一意の

認証コードが存在し、その認証コードは、その期間に加入を促される全てのユーザに対して有効とされる。登録に当たっては、機密認証コードと、この期間が、別個に（例えば、郵便あるいは口頭にて）携帯端末のユーザに知らせられる。携帯端末のユーザは、網に加入するためには、ユーザの機密認証コードを前記の期間内の日付に供給することを必要とされる。こうして、網コントローラは、ある与えられた瞬間（あるいは日付）に網の無線基地局に送られる認証コードが、その瞬間において要求される認証コードに等しいか否かを検証することのみを必要とされる。

【００１０】さらに、本発明は、移動電話標準ＤＥＣＴと完全にコンパティブルであるという長所を持つ。実際、前記システム、前記携帯端末、および前記登録方法が、推奨標準ＥＴＳＩ（欧州電気通信標準協会）３００１７５－４（以下の説明においてはＤＥＣＴ標準と呼ぶ）とコンパティブルな場合、前記機密認証コードが、前記標準の、１９９５年１月付けの第二版の段落１３．６に規定されるキー割当てと呼ばれる手続きにおける認証コードＡＣとして用いられる。

【００１１】本発明のもう一つの目的は、網コントローラが、データベース内でユーザが供給した認証コード、例えば、ユーザによって手操作にて生成されたコードと、登録リクエストの際に基地局に自動的に供給されるユーザ機器の番号（移動端末の通し番号）に割当てられたコードとが一致するか否かを検証する必要性を回避する、特に電話網のユーザを管理するための手段を提供することにある。

【００１２】これを達成するために、本発明の一つの実施例は、上述の電気通信システム、移動端末および登録法であって、前記端末が、識別番号あるいは通し番号、特にＤＥＣＴ標準に準拠するＩＰＥＩ（国際携帯機器識別）を持ち、前記機密認証コードが、移動端末のＩＰＥＩと独立なことを特徴とする。

【００１３】本発明のこれらおよびその他の特徴が、以下の実施例の説明から明らかとなるものである。

【００１４】

【発明の実施の形態】以下に、本発明の様々な実施例を、ＥＴＳＩ（欧州電気通信標準協会）によって定められるＤＥＣＴ（デジタル・エンハンスド・コードレス電気通信）移動電話技術標準との関連で説明する。ただし、本発明は、ユーザが網（ＣＴ２、ＥＴＡＣＳ、ＴＥＴＲＡ、ＧＳＭ等）に登録する際に、特に、ユーザがサービスに加入するに当たって、ユーザ認証手続きを必要とする任意の他の電気通信システムに適用できるものである。

【００１５】図１のシステムは、無線基地局１０を有する。この無線基地局１０は、カバレッジエリア１１を持ち、このカバレッジエリア１１の内側で、例えば、２つの移動端末１２と１３が移動する。これら移動端末１２と１３は、基地局１０と無線接続され、基地局１０は、ケーブル１６によって公衆交換電話網１５に接続される。

【００１６】他の幾つかの電気通信システムの例が、Philips Telecommunication Review,vol,52,no.3,January 1995において公表されている“コードレス・アクセスに対する完全な解決(The complete solution for cordless access)”なる文献において説明されている。

【００１７】本発明は、特に、移動無線端末を電気通信網に登録する手続きに関する。端末を最初に基地局に登録する際に、例えば、端末を購入し、移動端末のオペレータが、サービスに加入する場合、ユーザは、ユーザの識別を、基地局に認証メッセージを送ることで証明することが必要となる。

【００１８】ＤＥＣＴ（デジタル・エンハンスド・コードレス電気通信）標準は、ユーザが最初に網に登録する際に、ユーザが本人であることを確認するためのキー割当てと呼ばれる認証手続きを規定する。他方、各移動電話のオペレータは、携帯電話の製造業者と、加入者の機密認証コードを計算するための計算方法、およびこれら認証コードを含むデータベースを管理する方法について定義する必要がある。

【００１９】移動端末を電気通信網に登録するための周知の加入方法を図２に簡略的に示す。各移動端末２０は、ＤＥＣＴ（デジタル・エンハンスド・コードレス電気通信）標準においてＩＰＥＩと呼ばれる通し番号に対応する一意の認証番号を持つ。基地局２２は、端末２０の側から登録リクエスト２４を受信する。このリクエスト２４は、基地局２２に、移動端末を識別するための（特に、盗難端末でないことを識別するための）ＩＰＥＩ番号、および、加入したユーザを識別するための機密認証コードＡＣを供給する。

【００２０】制御ユニット２６は、加入者の機密認証コードＡＣの全リストとそれに対応するＩＰＥＩ番号とを有するデータベース２７の検証を遂行し、供給された機密認証コードＡＣが、受信されたＩＰＥＩに割当てられたリスト内にも含まれるか否か調べる。含まれる場合は、基地局２２は、端末２０の登録に移る。

【００２１】この登録手続きには、機密認証コードＡＣと携帯端末のＩＰＥＩの間の依存性のために、長い数のリストを管理し、多数の比較テストを遂行することが要求される。この手続きを簡素化し、網のデータベースへの多数のアクセスを回避するために、本発明による新規な方法においては、機密認証コードＡＣに、期間を割当てることで機密認証コードＡＣとＩＰＥＩの間の独立性が確保される。

【００２２】図３は、本発明による移動端末ＰＴを無線基地局ＦＴを介して電気通信網に登録するための加入手続きのステップを簡略的に示すが、このステップは、ＤＥＣＴ標準において規定されるキー割当てと呼ばれる手

続きによって実行される。

【００２３】無線基地局ＦＴは、移動端末ＰＴに対して、他の情報と共に、特に、用いられるべき機密認証コードＡＣの番号（あるいはタイプ）を含む“key_allocate”タイプのメッセージを送る。実際の使用に当たっては、各網あるいは各加入項目別に、機密認証コードＡＣにタイプが割当てられる。移動端末ＰＴは、無線基地局ＦＴに応答して、ＡＣ：ＡＣ1に基づいて得られる計算結果ＲＥＳ１を含む“authentication_request”タイプのリクエストを送り返す。無線基地局ＦＴは、この“authentication_request”メッセージを受信すると、移動端末ＰＴと同一の計算を、期待される機密認証コードＡＣ、すなわち、機密認証コードＡＣ2を利用して遂行することで結果ＸＲＥＳ１を得る。ＲＥＳ１＝ＸＲＥＳ１の場合は、移動端末ＰＴが認証される。この場合は、今度は、無線基地局ＦＴが、移動端末ＰＴによって認証されることが必要となる。従って、無線基地局ＦＴは、移動端末ＰＴに向けて、計算結果ＲＥＳ２を含む“authentication_reply”タイプのメッセージを送る。移動端末ＰＴは、このメッセージを受信すると、同一の計算を遂行し、結果ＸＲＥＳ２を得る。ＲＥＳ２＝ＸＲＥＳ２の場合は、無線基地局ＦＴが認証される。

【００２４】これら認証結果ＲＥＳ１、ＸＲＥＳ１、ＲＥＳ２およびＸＲＥＳ２は、推奨標準ＥＴＳＩ　３００１７５－７に準拠して計算される。機密認証コードＡＣをランダムに生成された他のデータと結合し、これをＤＳＡＡ（ＤＥＣＴ標準の認証アルゴリズム）の計算ユニットに加えることによって、上述の計算結果が得られる。

【００２５】本発明による一つの好ましい実施例においては、ある期間に割当てられた機密認証コードＡＣは、その期間内の瞬間（あるいは日付）に基地局に通信されることを意図される。この期間は、ユーザにとって加入手続きが可能な十分な長さに定められる。

【００２６】こうして、無線基地局によって期待され、ＸＲＥＳ１およびＲＥＳ２を計算するために用いられる機密認証コードＡＣ2は、現在の機密認証コードＡＣに対応しており、現在の機密認証コードＡＣは、所定の期間内の日付に加入することが促される全てのユーザに対して有効であり、現在の手続きはこの期間内に遂行されることを要求される。

【００２７】上述の移動端末ＰＴと無線基地局ＦＴの間の二重の認証が通過すると、網コントローラは、ＡＣ１＝ＡＣ2であるという結論を得、従って、生成されたコードが期待されるコードであるという結論に達し、携帯端末の登録が受理される。反対に、二重の認証が通過しなかった場合は、登録は拒絶される。

【００２８】図４の流れ図は、移動端末を、ＤＥＣＴ標準に準拠して、電気通信網に登録するための本発明の好ましい実施例に従う加入方法をより詳細に示す流れ図である。

【００２９】ボックスＫ０において、無線基地局ＦＴは、機密認証コードＡＣ、それに割当てられた期間τ、および多数のメッセージ内でパラメータとして用いられるユーザパーソナル識別ＵＰＩを決定する。

【００３０】ボックスＫ１において、こうして決定されたデータが、移動端末ＰＴのユーザに、Ｅ－メール、ファックス、あるいは通常の郵便の形式にて送られる。

【００３１】ボックスＫ２において、移動端末ＰＴが機密認証コードＡＣおよびユーザパーソナル識別ＵＰＩを含むＥ－メールを受信する。

【００３２】ボックスＫ３において、移動端末ＰＴは、加入リクエストを準備し、これを、無線にて無線基地局ＦＴに、特に機密認証コードＡＣを含む“access_right_request”タイプのメッセージとして送る。

【００３３】ボックスＫ４において、無線基地局ＦＴは、移動端末ＰＴからの加入リクエストを受信し、メッセージの受信日付ｔを（好ましくは１秒の精度にて）記録する。

【００３４】ボックスＫ５およびＫ６において、移動端末ＰＴと無線基地局ＦＴが、キー割当てタイプの手続きの様々なメッセージを交換する。より詳細には、生成された機密認証コードＡＣが、登録された受信日付ｔに対して期待されるコードであるか検証される。

【００３５】ボックスＫ７（ｔ＜τであるか否かの判定）において、前のテストの結果がテストされ；ｔが生成された機密認証コードＡＣに割当てられた期間τ内に含まれる場合は、結果は、肯定であり、方法はボックスＫ８に進み、否定の場合は、方法は、ボックスＫ９に進む。

【００３６】ボックスＫ８において、結果が肯定であるために、無線基地局は、移動端末の加入を受理し、移動端末に、“アクセス権受諾（access_right_accept）”タイプのメッセージを送る。

【００３７】他方、ボックスＫ９においては、結果が否定であるために、無線基地局は、移動端末の加入を拒絶し、“アクセス権拒絶（access_right_reject）”タイプのメッセージを送る。ボックスＫ１０において、加入手続きが終了する。

【００３８】本発明は、上述の一例としての実施例に制限されるものではない。当業者においては、様々な、より具体的には、ユーザ機密認証コード（ＡＣ）および期間の割当てを決定するための方法に関してのバリエーションが明白である。実際、同一コードのさまざまな期間への割当ては、一日ベースであっても、数日ベースであっても良く；要するに、不当なユーザによってダイヤルされた機密認証コードが、偶然に、正当な期間内に起こる確率が十分に低いことのみが要求される。例えば、コードをある期間に割当てるためのランダム計算法を用いることも可能であり、これら実施の形態の全てのバリエ

ーションが本発明の範囲内に入るものである。

【図面の簡単な説明】

【図１】本発明による電気通信システムの一例を示す図。

【図２】コードレス電話網に移動端末を登録するための周知の方法を簡略的に示す図。

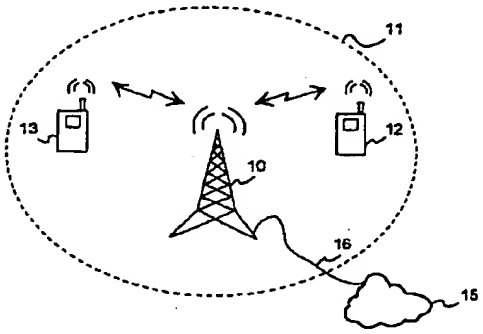
【図３】ＤＥＣＴ標準において規定されるキー割当てと呼ばれる手続きに適用された場合の本発明の方法を略図的に示す図。

【図４】本発明による登録方法の一例を流れ図にて示す図。

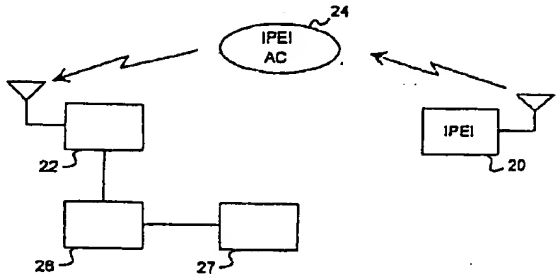
＊【符号の説明】

１０　無線基地局
１１　カバレッジエリア
１２、１３　移動端末
１５　公衆交換電話網
１６　ケーブル
２０　移動端末
２２　基地局
２４　登録リクエスト
２６　制御ユニット
２７　データベース

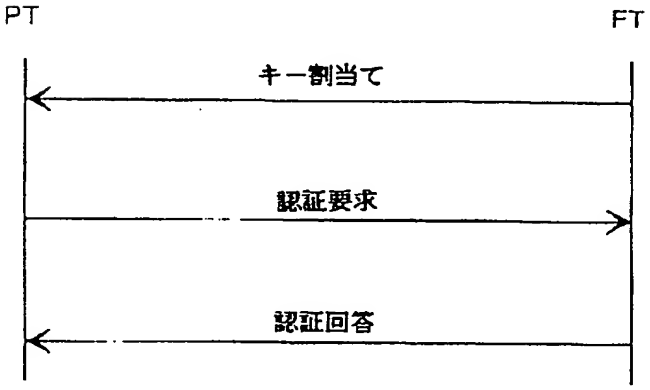
【図１】



【図２】



【図３】



【図４】